IN THE CLAIMS:

1. (currently amended) A method for conducting a consistent, documented and yet repeatable compliance risk assessment and mitigation process, using a network-based system including a server system coupled to a centralized database and at least one client system, said method comprising the steps of:

storing in the database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business;

displaying a questionnaire on a client system associated with a person responsible for compliance with at least one functional area within the business, the questionnaire is transmitted from the server system to the client system of the compliance person and is generated using the compliance information stored within the database;

receiving at the server a response inputted by the compliance person to the displayed questionnaire;

processing the response to the displayed questionnaire at the server;

prioritizing compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance;

identifying, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes;

storing the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence ratings, and the detection ratings in the database;

calculating a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is ~~directly related to the current controls in place~~ a product of the severity rating, the occurrence rating, and the detection rating;

implementing risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs; and

creating at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions.

2. (previously presented) A method according to Claim 1 wherein said step of displaying a questionnaire further comprises the steps of:

developing a binary questionnaire;

assembling a cross functional team;

defining what constitutes a "yes" answer for each question in the binary questionnaire;

identifying and interviewing the persons responsible for compliance for the questionnaire answers;

compiling interview results; and

summarizing findings and reviewing final results with compliance and functional leaders.

3. (previously presented) A method according to Claim 1 wherein said step of prioritizing compliance risks further comprises the steps of:

identifying the compliance risks of at least one of business' processes, products, environment, and location; and

prioritizing the business' highest risks.

4. (original) A method according to Claim 1 wherein said step of identifying further comprise the steps of:

analyzing identified high compliance risk areas to determine potential compliance failures and root causes; and

prioritizing actions that need to be taken; and

developing policy scorecards to be used as a monitoring and reporting tool.

5. (currently amended) A method according to Claim 1 wherein said step of identifying further comprises the steps of:

assembling a cross functional team;

mapping high risk process steps;

beginning a construction of a Failure Mode in Effect Analysis (FMEA);

assigning the severity, occurrence, and detection ratings based on a standard rating;

defining recommended actions to reduce the RPNs; and

determining scorecard content and format.

6. (previously presented) A method according to Claim 1 wherein said step of ensuring that implementing risk monitoring and control mechanisms, further comprises the steps of:

establishing appropriate controls to provide guidance to the business; and

monitoring that the appropriate controls to mitigate compliance risks.

7. (previously presented) A method according to Claim 1 wherein said step of implementing risk monitoring and control mechanisms are in place, further comprises the steps of:

developing action items;

ensuring that the developed action items are completed in a timely manner; and

establishing and monitoring the controls to mitigate compliance risks.

8. (previously presented) A method according to Claim 2 wherein said step of identifying and interviewing the persons responsible for compliance further comprises the steps of:

identifying and interviewing for compliance using a knowledge base; and

identifying and interviewing for compliance using a question owner's matrix.

9. (original) A method according to Claim 2 wherein said step of compiling interview results further comprises the step of compiling interview results using a spreadsheet configured for automatically converting the results from qualitative to quantitative and further configured to tabulate and graph the results.

10. (original) A method according to Claim 2 wherein said step of summarizing findings further comprises the step of summarizing the results of the assessment of at least one compliance program using at least one of a program assessment summary and a policy assessment summary.

11. (currently amended) A method according to Claim 3 wherein said step of prioritizing the business' highest [[risk]] <u>risks</u> further comprises:

mapping a high level business risk model;

compiling a list of compliance requirements from the compliance requirements stored in the database;

beginning construction of a quality function deployment (QFD) matrix;

assessing and evaluating compliance policies;

identifying immediate risks and completing constructing of a QFD matrix; and

prioritizing compliance risk areas associated with the business' highest risks.

12. (original) A method according to Claim 11 wherein said step of mapping the high level business risk model further comprises the steps of:

identifying core processes and products of a business;

associating business risk with the core processes and products of a business; and

associating business risk with compliance requirements.

13. (original) A method according to Claim 11 wherein said step of compiling a list of compliance requirements further comprises the step of compiling a list of compliance requirements including at least one of a company declared policy and/or practice, legal and regulatory requirements of a business, contractual requirements, compliance risks and internal requirements.

14. (original) A method according to Claim 11 wherein said step of prioritizing the list of compliance requirements further comprises prioritizing the severity level of non-compliance using a severity matrix.

15. (original) A method according to Claim 11 wherein said step of beginning construction of the quality function deployment (QFD) further comprises the steps of:

beginning construction of the QFD using information generated in mapping the high level business risk model with a compliance requirements list developed in making a severity matrix; and

quantifying the results using a risk QFD matrix.

16. (previously presented) A method according to Claim 11 wherein said step of assessing and evaluating compliance policies further comprises the steps of:

assessing business routines and controls to ensure compliance with each policy; and

determining a quality function deployment (QFD) score.

17. (original) A method according to Claim 16 wherein said step of determining a quality function deployment (QFD) score further comprises the step of determining a QFD score as

process strength rating × severity rating.

18. (original) A method according to Claim 16 wherein said step of determining a quality function deployment (QFD) score further comprises automatically entering the score into a risk QFD.

19. (original) A method according to Claim 11 wherein said step of prioritizing risk areas further comprises summarizing findings from the risk quality function deployment (QFD) using a risk prioritization matrix.

20. (original) A method according to Claim 11 further comprising the step of identifying the top three to five compliance requirements having the highest risk.

21. (previously presented) A method according to Claim 5 wherein said step of mapping the high-risk process steps comprises the steps of:

creating a first process map; and

creating a second process map within a failure mode and effect analysis matrix.

22. (original) A method according to Claim 5 wherein said step of beginning the construction of a failure mode and effect analysis matrix further comprises the steps of determining potential failure modes for each step in a process, brainstorming potential effects of the failure identifying potential causes of the failures and documenting current controls.

23. (previously presented) A method according to Claim 5 wherein said step of assigning severity, occurrence and detection factors further comprises automatically entering the assigned factors into a failure mode and effect analysis matrix.

24. (original) A method according to Claim 5 wherein said step of determining risk prioritization numbers further comprises determining the risk prioritization numbers as

severity rating × occurrence rating × detection rating.

25. (original) A method according to Claim 5 wherein said step of defining recommended actions to reduce the risk prioritization numbers further includes the step of automatically entering at least one of the recommended actions, an owner of the recommended action and expected date of completion of the recommended action into the failure mode and effect analysis matrix.

26. (canceled)

27. (original) A method according to Claim 5 further comprising the step of monitoring progress in reducing the risk prioritization numbers.

28. (original) A method according to Claim 27 wherein the step of monitoring progress in reducing the risk prioritization numbers comprises monitoring progress in reducing the risk prioritization numbers using policy scorecards.

29. (canceled)

30. (original) A method according to Claim 1 further comprising the step of monitoring metrics relating to training.

31. (currently amended) A system for identifying and quantifying compliance comprising:

at least one computer;

a database for storing compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business;

a server; and

a network connecting said computer to said server, wherein said server configured to display a questionnaire on said computer associated with a person responsible for compliance with at least one functional area within the business, said network is configured to transmit the questionnaire from said server to said computer of the compliance person and is generated using the compliance information stored within the database, said server is configured to:

receive a response inputted by the compliance person to the displayed questionnaire;

process the response to the displayed questionnaire;

prioritize compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance;

identify, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes;

store the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence rating, and the detection ratings in the database;

calculate a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is ~~directly related to the current controls in place~~ a product of the severity rating, the occurrence rating, and the detection rating;

recommend risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs; and

create at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions.

32. (previously presented) A system according to Claim 31 wherein said server is further configured to assemble a cross functional team, identify and interview for compliance, compile interview results and summarize the results of the assessment of at least one compliance program.

33. (original) A system according to Claim 32 wherein said server configured to assemble a cross-functional team is configured to assemble a cross-functional team using a knowledge base within said server.

34. (previously presented) A system according to Claim 32 wherein said server configured to assemble the cross-functional team using a knowledge base is further configured to create a questionnaire that includes a plurality of binary questions relating to compliance and define what constitutes an affirmative answer to the questions.

35. (original) A system according to Claim 32 wherein said server configured to identify and interview for compliance is configured to identify and interview for compliance using a knowledge base within said server.

36. (original) A system according to Claim 35 wherein said server configured to identify and interview for compliance is further configured to identify and interview for compliance using a question owner's matrix.

37. (original) A system according to Claim 32 wherein said server configured to compile interview results using a spreadsheet is configured to compile interview results using a spreadsheet configured for automatically converting results from qualitative to quantitative and to tabulate and graph results.

38. (original) A system according to Claim 32 wherein said server configured to summarize the results of the assessment is configured to summarize the results of the assessment using at least one of a program assessment summary and a policy assessment summary.

39. (previously presented) A system according to Claim 31 wherein said server configured to prioritize the risk is further configured to map a high level business risk model, compile a list of compliance requirements, prioritize the list of compliance requirements, construct a quality function deployment (QFD) matrix, assign a severity rating for non-compliance with requirements, assess and evaluate compliance policies.

40. (original) A system according to Claim 39 wherein said server configured to map the high level business risk model is further configured to identify at least one core process and product of a business, associate business risk with at least one core process and product of a business and associate business risk with compliance requirements.

41. (original) A system according to Claim 39 wherein said server configured to compile a list of compliance requirements is configured to compile a list of compliance requirements including at least one of a company declared policy and/or practice, legal and regulatory requirements of a business, contractual requirements, compliance risks and internal requirements.

42. (original) A system according to Claim 39 wherein said server configured to prioritize the list of company requirements is configured to prioritize the severity level of each occurrence of non-compliance in accordance with a severity matrix.

43. (original) A system according to Claim 39 wherein said server configured to construct the quality function deployment (QFD) matrix is further configured to construct the QFD matrix using information generated in mapping the high level business risk model with the compliance requirements list developed in creating a severity matrix.

44. (original) A system according to Claim 39 wherein said server configured to construct the quality function deployment (QFD) matrix is configured to quantify results using a risk QFD matrix.

45. (original) A system according to Claim 39 wherein said server configured to assess and evaluate compliance policies is configured to assess business routines and controls to ensure compliance with each policy and determine a quality function deployment (QFD) score.

46. (original) A system according to Claim 45 wherein said server configured to determine a quality function deployment (QFD) score is configured determine a QFD score as

process strength rating × severity rating.

47. (original) A system according to Claim 45 wherein said server configured to determine a quality function deployment (QFD) score is further configured to automatically enter the QFD score into a risk QFD matrix.

48. (original) A system according to Claim 39 wherein said server configured to prioritize compliance risk areas is further configured to summarize findings from the risk quality function deployment (QFD) matrix in accordance with a risk prioritization matrix.

49. (original) A system according to Claim 39 wherein said server is further configured to identify the top three to five compliance requirements having the highest risk.

50. (previously presented) A system according to Claim 31 wherein said server configured to identify issues relating to risk is further configured to assemble the cross-functional team, map the high risk process steps, construct a failure mode and effect analysis matrix, assign severity, occurrence and detection factors, determine risk prioritization numbers and define recommended actions to reduce the risk prioritization numbers.

51. (previously presented) A system according to Claim 50 wherein said server configured to map the high-risk process steps is further configured to create a first process map.

52. (previously presented) A system according to Claim 50 wherein said server configured to create a second process map is configured to create a process map in accordance with a failure mode and effect analysis matrix.

53. (original) A system according to Claim 50 wherein said server configured to construct a failure mode and effect analysis matrix is further configured to determine potential failure modes for each step in a process, brainstorm potential effects of the failures to identify potential causes of the failures and documents current controls.

54. (original) A system according to Claim 50 wherein said server configured to determine risk prioritization number is configured to determine risk prioritization numbers as

severity rating × occurrence rating × detection rating.

55. (original) A system according to Claim 50 wherein said server configured to assign a severity rating, occurrence and detection factors is further configured to enter the assigned factors into the failure mode and effect analysis matrix.

56. (original) A system according to Claim 50 wherein said server configured to define recommended actions is further configured to automatically enter at least one of the recommended actions, an owner of the recommended action, and expected date of completion of the recommended action into the failure mode and effect analysis matrix.

57. (canceled)

58. (original) A system according to Claim 50 wherein said server is further configured to monitor progress in reducing the risk prioritization numbers using policy scorecards.

59. (canceled)

60. (original) A system according to Claim 31 wherein said server is configured to allow a user to submit information relating to the identification and quantification of compliance via the Internet.

61. (original) A system according to Claim 31 wherein said server is configured to allow a user to submit information relating to the identification and quantification of compliance via an Intranet.

62. (original) A system according to Claim 31 wherein said network is one of a wide area network and a local area network.

63. (currently amended) A computer programmed to:

store in a database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business;

display a questionnaire for a person responsible for compliance with at least one functional area within the business, the questionnaire is generated using the compliance information stored within the database;

receive a response inputted by the compliance person to the displayed questionnaire;

process the response to the displayed questionnaire;

prioritize compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance;

identify, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of occurrence of the potential compliance failure modes the detection rating is a value representing whether current controls in place will detect potential compliance failure modes;

store the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, the occurrence ratings, and the detection ratings in the database;

calculate a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is ~~directly related to the current controls in place~~ a product of the severity rating, the occurrence rating, and the detection rating;

recommend risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs; and

create at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions.

64. (original) A computer according to Claim 63 further programmed to prompt a user to identify process owners within the compliance program.

65. (original) A computer according to Claim 63 wherein to identify the risks and failure modes and root causes, said computer displays a computer generated screen comprising a questionnaire relating to compliance.

66. (original) A computer according to Claim 65 wherein the questionnaire comprises a question owners matrix.

67. (original) A computer according to Claim 66 wherein said question owners matrix comprises a listing of compliance assessment areas.

68. (original) A computer according to Claim 63 further programmed to calculate a percentage of compliance.

69. (original) A computer according to Claim 65, said computer further programmed to tabulate and graph questionnaire results.

70. (previously presented) A computer according to Claim 63 wherein to prompt a user with a mitigation plan, said computer displays a computer generated screen comprising at least one of a completed questionnaire, a summary of current status, a plurality of improvement opportunities, a plurality of action plans and potential best practices, a program summary and a policy assessment summary.

71. (original) A computer according to Claim 63 wherein to prioritize the risks said computer is programmed to:

assess compliance risk; and

relate risks to processes, products and environments.

72. (original) A computer according to Claim 63 wherein to prioritize the risks said computer is programmed to prioritize a list of compliance requirements based upon a severity of non-compliance.

73. (original) A computer according to Claim 72 further programmed to organize the list of compliance requirements using a severity matrix format.

74. (original) A computer according to Claim 72 further programmed to generate a risk quality function deployment matrix, using compliance requirements and severity ratings for non-compliance of each compliance requirement.

75. (canceled)

76. (currently amended) A computer program embodied on a computer readable medium for managing compliance risk assessment to enable businesses to develop broader and deeper coverage of compliance risks, using a network based system including a server system coupled to a centralized database and at least one client system, said computer program comprising a code segment that:

stores in the database compliance information including at least one questionnaire relating to compliance, compliance requirements for each functional area within a business, and persons responsible for compliance within each functional area within the business;

displays a questionnaire on a client system associated with a person responsible for compliance with at least one functional area within the business, the questionnaire is transmitted from the server system to the client system of the compliance person and is generated using the compliance information stored within the database;

receives a response inputted by the compliance person to the displayed questionnaire;

processes the response to the displayed questionnaire at the server;

prioritizes compliance risks for the business including identifying compliance risks for each functional area within the business, and prioritizing the compliance risks from high to low based on a severity rating of non-compliance;

identifies, for each compliance risk identified, potential compliance failure modes, potential causes and effects of such compliance failure modes, current controls in place, an occurrence rating, and a detection rating, wherein the occurrence rating is a value representing a likelihood of the potential compliance failure modes and the detection rating is a value representing whether current controls in place will detect potential compliance failure modes;

stores the risks, the risk priority, the failure modes, the causes and effects of the failure modes, the current controls in place, occurrence ratings, and detection ratings in the database;

calculates a risk prioritization number (RPN) for each compliance risk identified based on the data stored in the database, wherein the RPN represents a relative compliance risk of a particular failure mode and is ~~directly related to the current controls in place~~ a product of the severity rating, the occurrence rating, and the detection rating;

recommends risk monitoring and control mechanisms to mitigate compliance risks based on the calculated RPNs including recommending actions to be implemented to reduce the calculated RPNs; and

creates at least one policy dashboard summarizing actions to be taken based on the recommended actions and key metrics for monitoring the implementation of the actions.

77. (original) The computer program as recited in Claim 76 further comprising a code segment that compiles list of compliance requirements and prioritizes list of compliance requirements based on relative severity of non-compliance.

78. (original) The computer program as recited in Claim 77 further comprising a code segment that compiles list of compliance requirements based on at least one of Regulatory Requirements, Contractual Requirements, Internal Policy Requirements and Spirit/ Letter Requirements.

79. (original) The computer program as recited in Claim 77 further comprising a code segment that:

stores severity rating for non-compliance requirements;

accesses strength of business routines and controls to ensure compliance with each policy;

computes a QFD score; and

prioritizes compliance risk areas according to risk criteria and process control strengths.

80. (original) The computer program as recited in Claim 79 further comprising a code segment that links business's core process to key compliance risks.

81. (original) The computer program as recited in Claim 76 further comprising a code segment that summarizes findings in an easily readable graphical and table formats.

82. (original) The computer program as recited in Claim 79 further comprising a code segment that:

reports progress since last review;

identifies focus areas for next review and defines specific recommended steps that business managers can implement to reduce risks.

83. (original) The computer program as recited in Claim 76 further comprising a code segment that generates management reports for at least one of business groups, departments, regions, and countries.

84. (original) The computer program as recited in Claim 76 further comprising a code segment that identifies opportunities for each businesses.

85. (original) The computer program as recited in Claim 76 wherein the network is a wide area network operable using a protocol including at least one of TCP/IP and IPX.

86. (original) The computer program as recited in Claim 76 wherein the data is received from the user via a graphical user interface.

87. (original) The computer program as recited in Claim 76 further comprising a code segment that develops questionnaires based on pre-stored assumptions in the database.

88. (original) The computer program as recited in Claim 76 wherein the client system and the server system are connected via a network and wherein the network is one of a wide area network, a local area network, an intranet and the Internet.

89. (original) The computer program as recited in Claim 76, and further comprising a code segment that monitors the security of the system by restricting access to unauthorized individuals.

90.-118. (canceled)

119. (previously presented) A method according to Claim 1 wherein said step of implementing risk monitoring and control mechanisms further comprises the steps of:

monitoring the status of a recommended action for a compliance risk;

determining whether the recommended action has been completed;

automatically reassigning a severity rating and a detection rating for the compliance risk associated with the completed recommended action; and

automatically recalculating the RPN for the compliance risk associated with the compliance risk associated with the completed recommended action.

120. (previously presented) A system according to Claim 31 wherein said server is further configured to:

receive updates regarding the status of a recommended action for a compliance risk;

determine whether the recommended action has been completed;

automatically reassign a severity rating and a detection rating for the compliance risk associated with the completed recommended action; and

automatically recalculate the RPN for the compliance risk associated with the completed recommended action.

121. (previously presented) A computer according to Claim 63 further programmed to:

receive updates regarding the status of a recommended action for a compliance risk;

determine whether the recommended action has been completed;

automatically reassign a severity rating and a detection rating for the compliance risk associated with the completed recommended action; and

automatically recalculate the RPN for the compliance risk associated with the completed recommended action.

122. (previously presented) The computer program as recited in Claim 76 further comprising a code segment that:

receives updates regarding the status of a recommended action for a compliance risk;

determines whether the recommended action has been completed;

automatically reassigns a severity rating and a detection rating for the compliance risk associated with the completed recommended action; and

automatically recalculates the RPN for the compliance risk associated with the completed recommended action.